



# ODNI/ONCIX

## Enterprise Performance Management Training and Assistance Group Course Descriptions

### PLEASE READ:

- *Contractors must provide on-site government support and have Government Supervisor or COTR email [ONCIX-Training@dni.gov](mailto:ONCIX-Training@dni.gov) with concurrence for attendance at time of registration and will be added to the general wait list for the course(s) requested.*
- *Clearance Information - You will receive notification on passing your clearances in your welcome packet approximately one month prior.*
- *Courses may have students from our Commonwealth Partner Countries; contact us if this may impact your attendance.*
- *Our courses are not certification courses for DSS*

**ATTENDANCE POLICY:** *Students are required to attend all scheduled days of training unless absence is excused by a course facilitator. Classes will begin promptly at 8:00am so please make sure you are familiar with the course location and that you arrive on time.*

### Privacy Notice:

*The information you provide enables the NCIX Training and Assistance Group (TAG) to process your request to participate in a course. It also enables TAG to respond to your inquiries regarding course completion and academic transcripts, should you require such information at a future time. Records are maintained by course title and date of delivery. No other use is made of information contained in registrants' course request forms. The emergency contact information you provide will be maintained securely and deleted upon course completion.*

### ICD 704 PERSONNEL SECURITY COURSE

**PURPOSE:** This course prepares you to make adjudicative decisions consistent with ICD 704 requirements. We will present approaches to enhance best practices and reciprocity across the Intelligence Community and DoD organizations authorized to grant access and adjudicate for Sensitive Compartmented Information. We will explain the adjudication process and identify what should be considered to upgrade an individual to another clearance and/or access level. This is also an excellent seminar for security professionals who want to better understand the process behind adjudication decisions.

**LENGTH:** 5 days / 8:00 - 4:30 (8:00 - 12:30 on Friday)

**TARGET:** Personnel performing background checks, clearance upgrades and adjudications. This course is also appropriate to enhance knowledge of the well-rounded career security professional.

### PREREQ:

#### **SECRET clearance**

- Please review ICD 704 prior to attending course.

## ICD 705 PHYSICAL SECURITY COURSE

**PURPOSE:** The ICD 705 Physical Security Course: Lifecycle of A SCIF will prepare you to implement the requirements of the new ICD 705 series documents (ICD 705; ICS 705-1; ICS 705-2 and the ICD 705 Technical Specifications). The course is designed using a SCIF lifecycle theme:

- Phase I: Threat Definition and Planning
- Phase II: Preliminary Construction Planning
- Phase III: Design and Construction Requirements
- Phase IV: Accreditation
- Phase V: SCIF Operations and Management
- Phase VI: Disposal of a SCIF

The course stresses comprehension and construction best practices and application of the ICD 705 series documents. The course ends with an Intelligence Community (IC) Forum. The forum is comprised of senior leaders, accreditors and inspectors from across the IC.

**LENGTH:** 5 days / 8:00 - 4:30 (8:00 - 12:30 on Friday)

**TARGET:** Federal government civilians, military personnel and government contractors responsible for the physical planning and implementation of SCI and SAP facilities.

**MATERIALS:** UNCLASSIFIED w/classified discussions

**PREREQ:**

- **SECRET clearance**
- Please review the following documents prior to course attendance:
  - IC Directive 705, Sensitive Compartmented Information Facilities (SCIFs)
  - IC Standard 705-1, Physical and Technical Standards for SCIFs
  - IC Standard 705-2, Standards for Accreditation and Reciprocal Use of SCIFs

## SPECIAL SECURITY OFFICER COURSE (SSOC)

**PURPOSE:** Prepare security professionals who administer SCI programs. We will familiarize you with security ICDs and SCI policies and compartments. We use practical implementation exercises to give hands-on experience. The topics include:

- Structure of Intelligence Community
- Security Incidents and Investigations
- Business and Security Interfaces
- Security Awareness, Training, and Education Programs
- Special Access Programs
- Physical Security (ICD 705)
- Personnel Security (ICD 704)
- Information Systems Security (ICD 503)

**LENGTH:** 5 days / 8:00 - 4:30 (8:00 - 12:30 on Friday)

**TARGET:** Security professionals who administer all aspects of SCI programs

**PREREQ:**

- **Secret Clearance**
- Recommended that they have 2-5 years security experience

## PRINCIPLES OF INSIDER THREAT PROGRAM AND OPERATIONS COURSE

**PURPOSE:** This is a revised course that consolidates the Establish and Operate an Insider Threat course and the Principles of Hub Operations course and is designed to expose Insider Threat personnel to current issues and perspectives that prepare them to establish their Insider Threat Programs and operate their Insider Threat Hub. This course contains practical implementation exercises to give hands-on experience. The class is divided into teams with an assigned instructor/facilitator for individual attention. The topics include:

- How to meet the requirements of EO 13587, which directs US Government executive branch departments and agencies to establish, implement, monitor, and report on effectiveness of insider threat programs to protect classified national security information.
- Identify your agency's gaps in CI and security
- Do a mock Risk Assessment for your Agency
- Drafting your Implementation Plan
- Drafting an Insider Threat Program Policy
- Insider Threat Program Hub
- Hub Functions
- Manual/Auto Aggregation of Data Sources
- Case Management
- Inquiries
- Responses and Referrals
- Hearing "Voices from the Field" and how they worked to get their programs running. This will give you a practical view of what that looks like in a budget constrained environment.
- Capstone Exercise

**LENGTH:** 3 days / 8:00 - 4:30

**TARGET:** Insider Threat Personnel and/or designated officials

**MATERIALS:** **SECRET/NOFORN**

- **PREREQ:** Insider Threat Program Manager/Senior Official must send e-mail concurrence to [ONCIX-Training@dni.gov](mailto:ONCIX-Training@dni.gov) for participant(s) enrollment at time of registration.

**OBJECTIVES:**

- Understand the requirements of the Executive Order
- Gain information, recommendations, and ideas on how these may be satisfied
- Build or be introduced to draft products required by the EO:
  - a) Risk Analysis
  - b) Implementation Plan and Policy
  - c) Insider Threat Awareness Training for the Workforce
- Understand the requirements of Hub Operations
- Describe the Hub Functions required to gather information, recommendations, and ideas on that support the Insider Threat Program.
- Identify the activities and requirements of:
  - a) User Activity Monitoring
  - b) Manual/Auto Aggregation of Data Sources
  - c) Case Management
  - d) Inquiries, Responses, and Referrals
  - e) Reporting
- Case Studies and Practical Exercises to Reinforce Learning

## NAME TRACE WORKSHOP

This workshop will be held on an as needed basis only.

**PURPOSE:** To expose counterintelligence and security professionals to available national level databases and resources for screening and vetting foreign nationals. During the workshop, participants will receive a current foreign intelligence collection threat briefing; a Department of Homeland Security (DHS) Foreign Access Management (FAM) program briefing; FBI National Name Check Program briefing and briefing from other applicable national level resources. There will also be live demonstrations using the Business Risk Analysis Clearinghouse (BRANCH) tool and other intelligence community applications.

**LENGTH:** 1 day, 8:00 - 4:00 (with an hour break for lunch)

**TARGET:** New or junior investigators, analysts, security officers, and adjudicators assigned to counterintelligence or security programs

**MATERIALS:** **SECRET//NOFORN**

**PREREQ:** None

**OBJECTIVES:**

- List key national and community name trace databases
- List available resources to validate a foreign national's identity
- Perform the basic mechanics of a name trace
- Define the meaning of "no record on file" type responses
- Explain the value of conducting name traces and vetting foreign nationals
- Case Studies and Practical Exercises to Reinforce Learning